UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,645	02/13/2001	Thomas Andrew Cocotis	19951/01201	2776

26116 7590 10/21/2004

SIDLEY AUSTIN BROWN & WOOD LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/782,645	COCOTIS ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/3/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 have been examined.

Specification

2. The abstract of the disclosure is objected to because it contains more than one paragraph and exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

Claim Objections

3. Claim 25 is objected to because of the following informalities: change "a list said files" (clause c) to "a list of said files". Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 3 and 5-6 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 3, it recites "a method of authenticating and verifying the integrity in accordance with claim 1" in the preamble; however, it is claim 2 that claim "a

method of authenticating and verifying the integrity of a content file". For examination purpose, claim 3 is treated as being dependent on claim 2.

6. Claims 5 and 6 recite the limitation "wherein the step of providing the client computer with a public key" in the 3rd-4th lines of each claim. There is insufficient antecedent basis for this limitation in the claims. The limitation "the step of providing the client computer with a public key" is introduced in claim 3. For examination purpose, claims 5 and 6 are treated as being dependent on claim 3.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

8. Claims 2, 4, 7-8 and 27 are rejected under 35 U.S.C. 102(a) as being anticipated by Wright et al (WO 00/59177).

a. Regarding claims 2 and 27, Wright discloses a method of authenticating and verifying the integrity of a content file delivered from a server computer to a client computer over a network, comprising the steps of:

registering a content file by generating unique registration information using a first key (fig. 2, steps 200-204);

storing the content file and the registration information on the server computer (p. 11, lines 1-3);

accessing the content file and the registration information in response to a request from the client computer (fig. 4, steps 400-404);

authenticating the integrity of the content file and the registration information accessed by the server computer by use of a second key (fig. 4, step 406); and

transmitting the authenticated content file and registration information to the client computer (fig. 4, step 408; p. 3, lines 8-32).

b. Regarding claim 4, Wright further discloses that the client computer can use the public key to generate registration information unique to the content file transmitted from the server computer and can validate the registration information generated using the public key relative to the registration information transmitted from the server computer (p. 5, lines 6-31).

c. Regarding claim 7, Wright further discloses that the step of registering a content file by generating unique registration information comprises generating a server digital signature of the content file, using the private key and storing the server digital signature along with a file name of the content file (fig. 2, step 204).

d. Regarding claim 8, Wright further discloses that the step authenticating the integrity of the content file and the registration information comprises validating the server digital signature accessed by the server computer, using the public key (fig. 4, step 406).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 26 and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borrowman et al. (2004/0039912 A1) in view of Wright. Borrowman discloses a method comprising:

registering a content file received at the computer, comprising:

generating a first digital signature of the content tile (fig. 10, step 1020);

generating a secondary digital signature of the first digital signature and a file name of the content file (paragraphs 0096-0097); and

storing the content file, the first digital signature, the file name, and the second digital signature (paragraphs 0091 and 0097);

accessing the stored content file, the stored first digital signature, the stored tile name, and the stored secondary digital signature (paragraphs 0094 and 0097);

validating the secondary digital signature of the stored content file (par. 0097).

Borrowman does not disclose generating the digital signatures using a first key and validating the digital signatures using a second key corresponding to the first key. Borrowman also does not disclose the step of validating the first digital signature of the stored content file. Wright discloses generating digital signatures using a public-key

algorithm (p. 5, lines 6-10) and validating a digital signature of a stored content file, which is equivalent to the first digital signature, at the time the content file is requested (fig. 4, step 406). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Borrowman method to generate the digital signatures using a public-key algorithm, as taught by Wright. Digital signature techniques using public key cryptography allow checks not only as to authentication but also as to integrity. Accordingly, the first key is a private key and the second key is a public key corresponding to the private key. It would also have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Borrowman method to validate the first digital signature of the stored content file, as taught by Wright, in order to determine if the stored content file has been tampered with (p. 7, line 15-24).

11. Claims 3 and 6 rejected under 35 U.S.C. 103(a) as being unpatentable over Wright as applied to claim 2 above, and further in view of Mueller et al. (6,351,816). Wright does not disclose providing the client with the server's public key. Mueller discloses providing a client with a digital certificate having the server's public key (col. 4, lines 17-22). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wright method to provide the client with a digital certificate having the server's public key so that the client could use the public key to verify the digital signature of the downloaded file (col. 3, lines 44-54).

12. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wright as applied to claim 3 above, and further in view of Nagai et al. (EP 0 982 927 A1). Wright does not disclose transmitting to the client computer a consumer application having the public key embedded therein. Nagai discloses transmitting to a client computer a consumer application having the public key embedded therein (par. 0038). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wright method to transmit to the client computer a consumer application having the public key embedded therein, as taught by Nagai. The consumer application has the public key needed to verify the digital signature of the content file downloaded to the client computer.

13. Claims 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright as applied to claim 7 above, and further in view of Borrowman. Wright only discloses generating a server digital signature using the private key and validating the server digital signature accessed by the server computer, using the public key (fig. 2, step 204; fig. 4, step 406). Wright does not disclose generating a secondary digital signature of the server digital signature of a file and the file name, storing and validating the secondary digital signature. Borrowman discloses generating a record for each registered file including a server digital signature of the file and the file name in a log file and generating a digital signature of the log file. The digital signature of the log file meets the limitation of a secondary digital signature of a server digital signature of a file and the file name. Borrowman also discloses storing and validating the digital signature

of the log file (paragraphs 0096-0097). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Wright to generate a secondary digital signature of the server digital signature and the file name, store and validate the secondary digital signature, as taught by Borrowman, in order to guard against tampering with the data included in the log file.

14. Claims 12 and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shaio (6,430,608) in view of Wright and Mueller. Shaio discloses a method of authenticating and verifying the integrity of content delivered over a public network in response to a request transmitted from a client computer to a server computer, comprising the steps of:

generating server validation information unique to each content tile (fig. 2, elements 256A-C);

assembling a primary list identifying each content file responsive to the client computer's request (col. 1, lines 30-36; fig. 2, elements 254A-C);

transmitting to the client computer the primary list and the server validation information associated with each content file identified in the primary list (fig. 3A, step 312);

authenticating and verifying any content files identified in the primary list which are already resident on the client computer, comprising the steps of:

assembling a matching list identifying each content file identified in the primary list which is stored on the client computer and a non-matching list identifying

each content file identified in the primary list which is not stored on the client computer (col.7, lines 56-60);

validating the server validation information received from the server computer for each content file identified in the matching list (col. 7, lines 56-67); and

removing from the matching list and adding to the non-matching list each content file identified in the matching list for which the server validation information is not successfully validated (col. 5, line 47 – col. 6, line 8; col. 7, lines 56-67);

transmitting to the client computer each content tile identified in the non-matching list (col. 5, line 66 – col. 6, line 8); and

validating the server validation information for each content file received from the server computer and identified in the non-matching list (col. 5, line 66 – col. 6, line 8; fig. 3A).

Shaio does not disclose providing the client computer with a public key corresponding to a private key maintained by the server computer. Mueller discloses providing a client with a digital certificate having the server's public key (col. 4, lines 17-22). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wright method to provide the client with a digital certificate having the server's public key so that the client could use the public key to verify the digital signature of the downloaded file (col. 3, lines 44-54).

Shaio discloses that the server validation information is a digital signature of a file (fig. 2C, elements 256A-C). However, Shaio does not disclose that that the digital signature is generated during a registration process using public-key cryptography.

Wright discloses generating server registration information unique to each content tile stored on the server computer. The server registration information is a digital signature of a file generated using a private key (fig. 2, steps 200-204) and used to verify that a file has not been tampered before the server transmits the file to the client (fig. 4, step 406). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Shaio method such that the digital signature is generated during a registration process using public-key cryptography, as taught by Wright. A digital signature of a file created in the registration process is used to determine whether the file has been tampered when being stored at the server (p. 7, lines 15-24). Digital signature techniques using public key cryptography allow checks not only as to authentication but also as to integrity (p. 5, lines 6-10).

15. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shaio, Wright and Mueller as applied to claim 12 above, and further in view of Nagai. Shaio, Wright and Mueller do not disclose transmitting to the client computer a consumer application having the public key embedded therein. Nagai discloses transmitting to a client computer a consumer application having the public key embedded therein (paragraphs 0010-0011). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Shaio, Wright and Mueller to transmit to the client computer a consumer application having the public key embedded therein, as taught by Nagai. The consumer application has the public

key needed to verify the digital signature of the content file downloaded to the client computer.

16. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shaio, Wright and Mueller as applied to claim 15 above, and further in view of Borrowman. In claim 15, Shaio, Wright and Mueller only discloses generating a server digital signature for each file stored at the server using the private key and validating the server digital signature of a requested file before transmitting the requested file to a client using the public key (fig. 2, step 204; fig. 4, step 406). Shaio, Wright and Mueller do not disclose generating a secondary digital signature of the server digital signature of a file and the file name, storing and validating the secondary digital signature. Borrowman discloses generating a record for each registered file including a server digital signature of the file and the file name in a log file and generating a digital signature of the log file. The digital signature of the log file meets the limitation of a secondary digital signature of a server digital signature of a file and the file name. Borrowman also discloses storing and validating the digital signature of the log file (paragraphs 0096-0097). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Shaio, Wright and Mueller to generate a secondary digital signature of the server digital signature and the file name, store and validate the secondary digital signature, as taught by Borrowman, in order to guard against tampering with the data included in the log file.

17. Claims 19-23, 28 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagai in view of Shaio.

a. Regarding claims 19, 28 and 31, Nagai discloses a method for requesting content from a server computer over a public network and displaying the content to a user on a client computer only after the integrity of such content has been authenticated and verified, comprising the steps of:

transmitting a request to the server computer for content necessary to build a displayable Web page (paragraphs 0010-0012);

receiving from the server computer the files necessary to build a displayable Web page and a server digital signature uniquely associated with the Web page (par. 0012; fig. 6);

validating the server digital signature for the Web page (fig. 7, step 604); and

if the server digital signature for the Web page is validated, displaying on the client computer the Web page (fig. 7, step 605).

The Nagai reference discloses transmitting multiple files necessary to build the requested Web page; however, only one digital signature for the files is generated at the server and verified at the client. Nagai does not disclose generating a digital signature for each individual file, transmitting a list of the file names and their associated digital signatures to the client for verification. Shaio discloses a method for generating and transmitting a manifest which is a list of the files to be transmitted and their associated digital signatures to the client (fig. 2C), and validating the digital signatures using the man the manifest at the client (fig. 3). In particular, Shaio discloses validating the server

digital signature for each file stored locally on the client computer which is identified in the list (col. 7, lines 56-65), transmitting to the server computer a secondary list identifying each file identified in the primary list which is not stored locally on the client computer or for which the server digital signature is not successfully validated (col. 4, lines 18-32; col. 5, line 47 – col. 6, line 8), receiving from the server computer each file identified in the secondary list (col. 6, lines 6-8 and 12-17); and validating the server digital signature for each file received from the server computer and identified in the secondary list (figures 2C and 3A). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Shaio method for generating and transmitting a manifest which is a list of the files to be transmitted and their associated digital signatures to the client, and validating the digital signatures of the files using the manifest at the client into the Nagai method. The Shaio manifest not only allows files to be validated and authenticated but can also be used in a wider variety of circumstances than a conventional manifest (col. 2, lines 8-10).

b. Regarding claim 20, Shaio further discloses deleting each file stored locally on the client computer for which the server digital signature is not successfully validated (col. 5, lines 60-66).

c. Regarding claim 21, Shaio further discloses displaying on the client computer an error message if the server digital signature is not successfully validated for any file received from the server computer and identified in the secondary list (col. 5, line 66 – col. 7, line 5).

d. Regarding claims 22-23, Shaio further discloses transmitting to the server computer an error list identifying each file identified in second list for which the server digital signature is not successfully validated (col. 4, lines 18-32; col. 5, line 47 – col. 6, line 8), receiving from the server computer each file identified in the error list (col. 6, lines 6-8 and 12-17); and validating the server digital signature for each file received from the server computer and identified in the secondary list (figures 2C and 3A).

18. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nagai in view of Borrowman, Wright and Shaio. Nagai discloses a system for delivering Web content from a server computer to a client computer over a public network and displaying the content on the client computer only after the integrity of such content has been authenticated and verified, comprising the steps of:

providing the client computer with a public key which corresponds to a private key maintained at the server computer (par. 0038; fig. 3);

transmitting from the client computer to the server computer a request for content necessary to build a displayable web page (paragraphs 0010-0012);

generating a server digital signature of the Web page using the private key (fig. 6);

transmitting from the server computer to the client computer the files necessary to build a displayable Web page and the server digital signature of the Web page (par. 0012; fig. 6); and

validating the server digital signature of the Web page, using the public key (fig. 7).

Nagai does not disclose generating the server digital signature of the Web page when the Web page is registered at the server and validating the digital signature at the server when the Web page is requested. Wright discloses generating the server digital signature of the Web page when the Web page is registered at the server and validating the digital signature at the server when the Web page is requested (figures 2 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Nagai system to generate the server digital signature of the Web page when the Web page is registered at the server and validate the digital signature at the server when the Web page is requested, as taught by Wright, in order to determine if the Web page has been tampered with at the server (p. 7, line 15-24).

Nagai does not disclose generating a secondary digital signature of the server digital signature and the corresponding file name and validating the secondary digital signature at the server when the Web page is requested. Borrowman discloses generating a secondary digital signature of a server digital signature of a file and the corresponding file name and validating the secondary digital signature at the server when the file is requested (paragraphs 0096-0097). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Nagai system to generate a secondary digital signature of the server digital signature and the corresponding file name and validating the secondary digital signature at the server

when the Web page is requested, as taught by Borrowman, in order to guard against tampering with data associated with the file.

Nagai discloses transmitting multiple files necessary to build the requested Web page; however, only one digital signature for the files is generated at the server and verified at the client. Nagai does not disclose generating a digital signature for each individual file, transmitting a list of the file names and their associated digital signatures to the client for verification. Shaio discloses a system for delivering content using a manifest which is a list of the files to be transmitted and their associated digital signatures to a client (fig. 2C), and validating the digital signatures using the man the manifest at the client (fig. 3). In particular, Shaio discloses assembling a matching list identifying each file in the manifest which is stored at the client and a non-matching list identifying each file in the manifest which is not stored a the client (col. 7, lines 56-60), validating the server digital signature for each file stored on the client computer and identified in the matching list (col. 7, lines 56-65), transmitting to the server computer non-matching list identifying each file not stored locally on the client computer or for which the server digital signature is not successfully validated (col. 4, lines 18-32; col. 5, line 47 – col. 6, line 8); and validating the server digital signature for each file received from the server computer and identified in the non-matching list (figures 2C and 3A). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Shaio system for generating and transmitting a manifest which is a list of the files to be transmitted and their associated digital signatures to the client, and validating the digital signatures of the files using the manifest at the client into the

Nagai system. The Shaio manifest not only allows files to be validated and authenticated but can also be used in a wider variety of circumstances than a conventional manifest (col. 2, lines 8-10).

19. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shaio in view of Wright. Shaio discloses a system for verification of file content which is transmitted from a sever to a client through a network, comprising:

said server having therein a server program for:

sending a list of files and associated digital signature for each file to said client (fig. 2C; fig. 3A, step 312),

sending the requested files to said client via said network (fig. 3A, step 310),

said client of said server having therein a client program for:

requesting said file content via said network (fig. 3A, step 310),

upon receiving said list of said files and said digital signatures, detecting the presence of any of said files on said list in local storage for said client (col. 7, lines 56-65),

for said local files, which are on said list and located in said local storage, verifying said local files by use of said digital signatures (col. 7, lines 56-65), and

requesting from said server the ones of said files on said list which were not verified by said client (col. 6, lines 6-8).

Shaio does not disclose generating the server digital signature of a file when the file is registered at the server. Wright discloses generating the server digital signature of a file when the file is registered at the server (figures 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Shaio system to generate the digital signature of a file when the file is registered at the server, as taught by Wright. The digital signature generated is used to determine if the file has been tampered with at the server (p. 7, line 15-24).

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Palage et al. (6,018,801) discloses a method for authenticating electronic documents on a computer network.

Groshon et al. (6,351,811) discloses systems and methods for preventing transmission of compromised data in a computer network.

Schneier ("Applied Cryptography") discloses different digital signature protocols.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
10/08/2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100